EMANUELE BOSIMINI

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Tecniche di difesa delle infrastrutture critiche con strumenti di decezione e piattaforme di monitoraggio

Tutor: Stefano Bistarelli

GIORNATA DI INCONTRO
BORSE DI STUDIO GARR
"ORIO CARLINI"
ROMA
21/04/2021

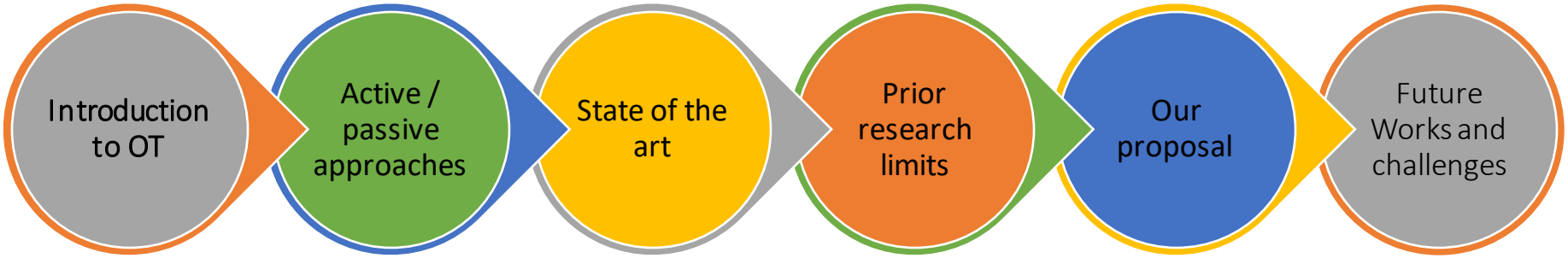
CyberSecurity Research Lab UniPG

Università degli Studi di Perugia

«All warfare is based on deception.»

— Sun Tzu

Summary


Introduction to OT
Active / passive approaches
State of the art
Prior research limits
Our proposal
Future Works and challenges

Summary

Introduction to OT

Active / passive approaches

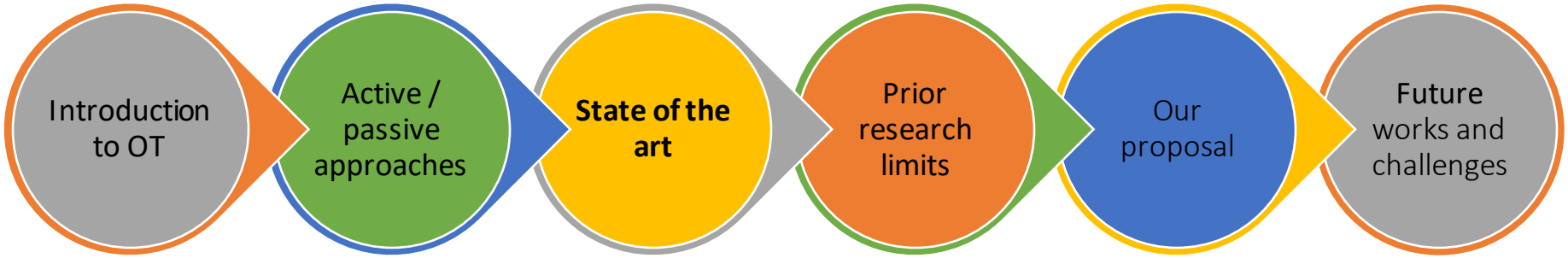
State of the art

Prior research limits

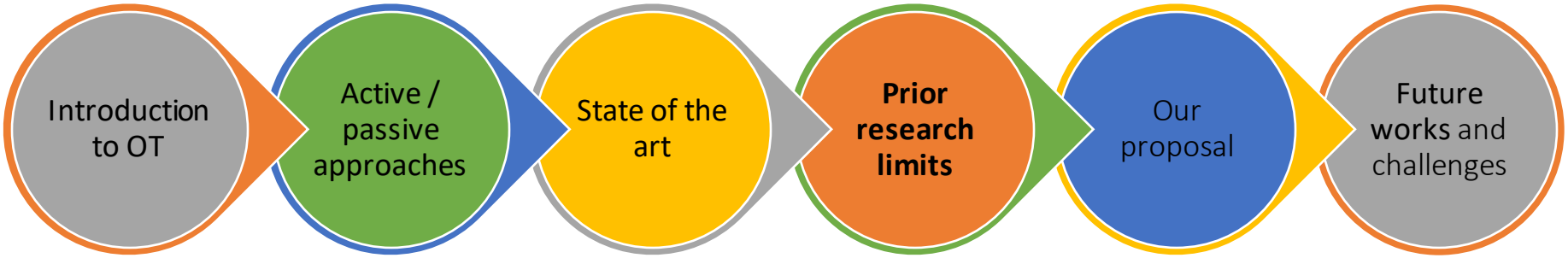
Our proposal

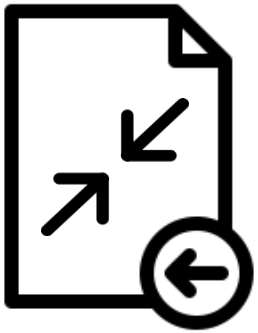
Future works and challenges

Summary

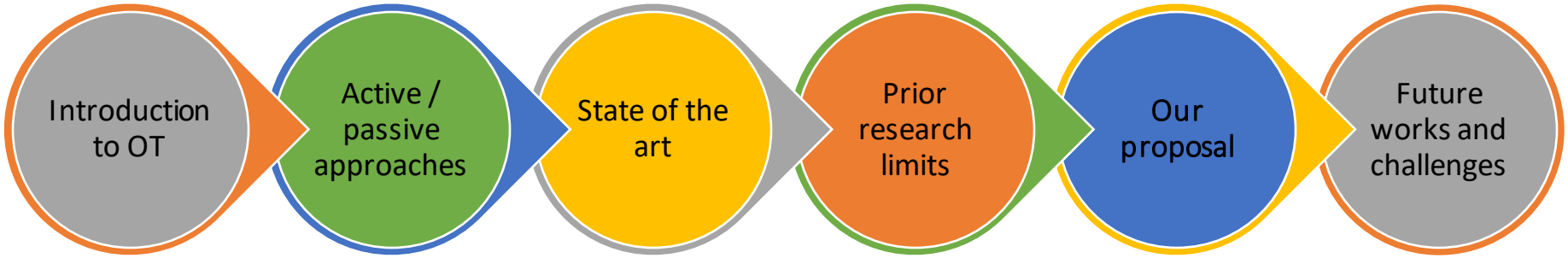

Introduction to OT
Active / passive approaches
State of the art
Prior research limits
Our proposal
Future works and challenges

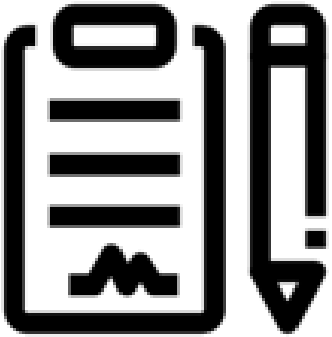
Summary


Introduction to OT
Active / passive approaches
State of the art
Prior research limits
Our proposal
Future works and challenges

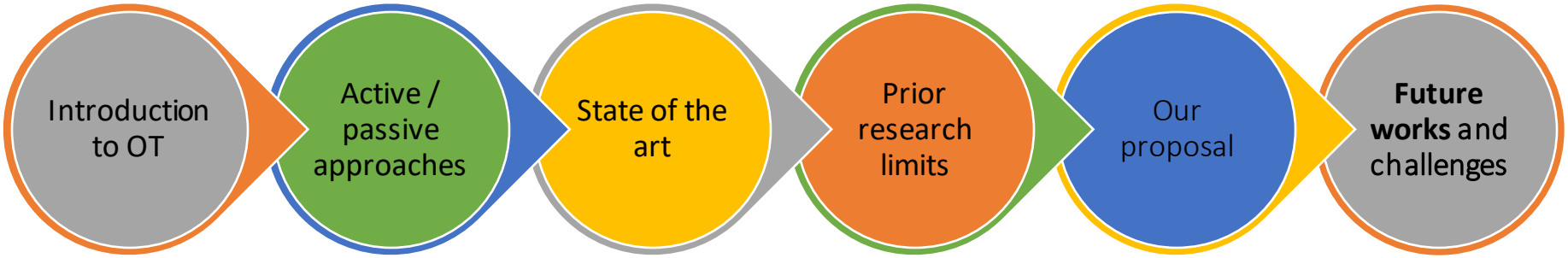


Summary


Introduction to OT
Active / passive approaches
State of the art
Prior research limits
Our proposal
Future works and challenges



Summary


Introduction to OT
Active / passive approaches
State of the art
Prior research limits
Our proposal
Future works and challenges

Operational Technology

Definition (NIST)

Hardware and software that **detects** or **causes** a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

(a) Doel Power Plant, Belgium (Credits: Nicholas Therpen).

(b) Power Pylons (Credits: Matthew Henry).

IT vs OT priorities

CIA

SAIC

OT security problems

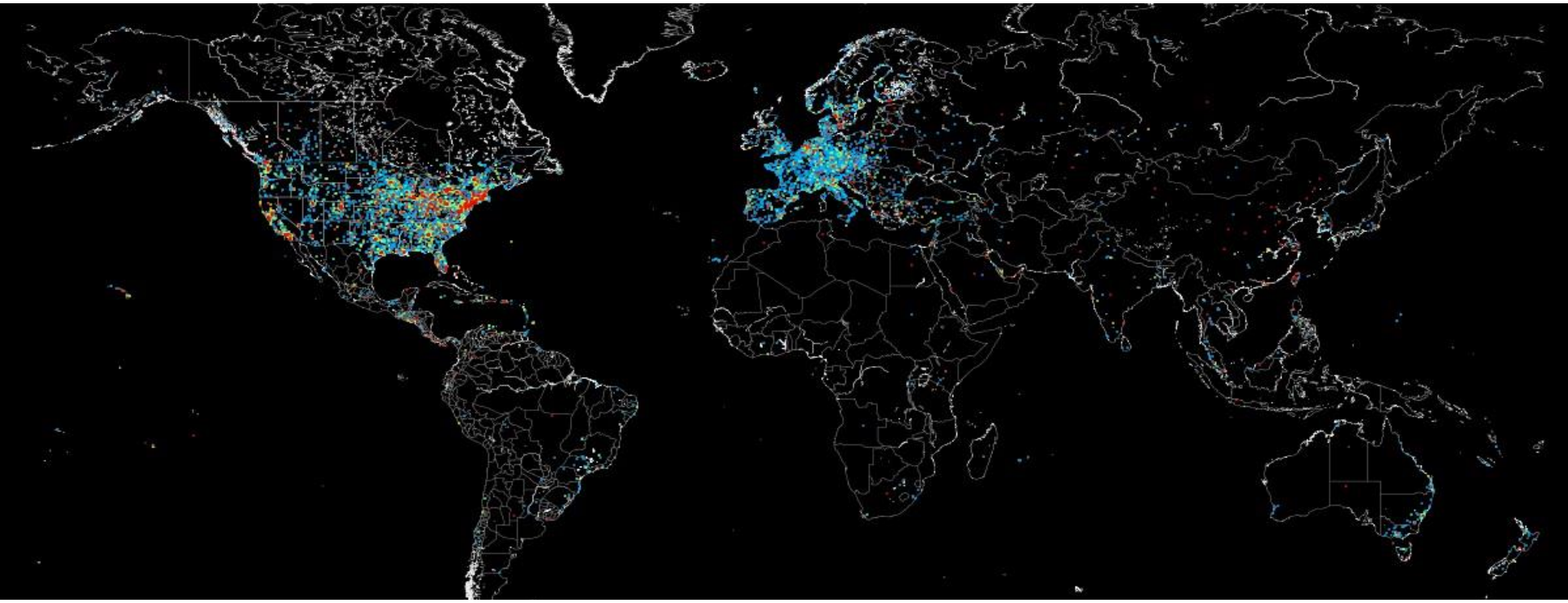
Company's perspective

- Firewall misconfigurations
- Host-based antivirus

Protocol's perspective

- Insecurity **by design**
- Treating OT protocols as IT protocols

Industrial devices exposure



Publicly exposed ICS to the Internet = **Vulnerable**

~23k Modbus

~48k Siemens, 30% **repeating** serial numbers

Approaches

Statistical analysis

- Network telescope (Darknet)
- Low-interaction honeypots

In-depth analysis

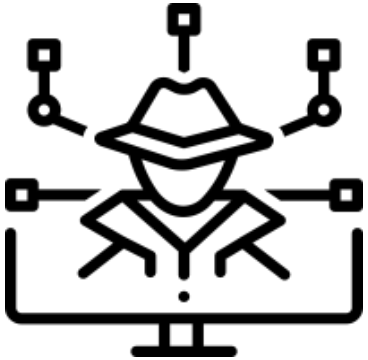
- Medium-Interaction honeypots
- High-Interaction honeypots

State of the art (Shrinked)

Honeypot	Interaction	Camouflage	Protocols	Extensibility
DiPot (Cao et al.)	Low	Not proven	HTTP, Modbus, S7comm, BACnet	Yes (XML)
Gaspot	Low	Detected	Port 10001	Yes
Conpot	Low	Detected	Skipped for brevity	Yes (XML)
SCADA Honeynet Project	Low	Not proven	Modbus, HTTP, FTP, Telnet	No

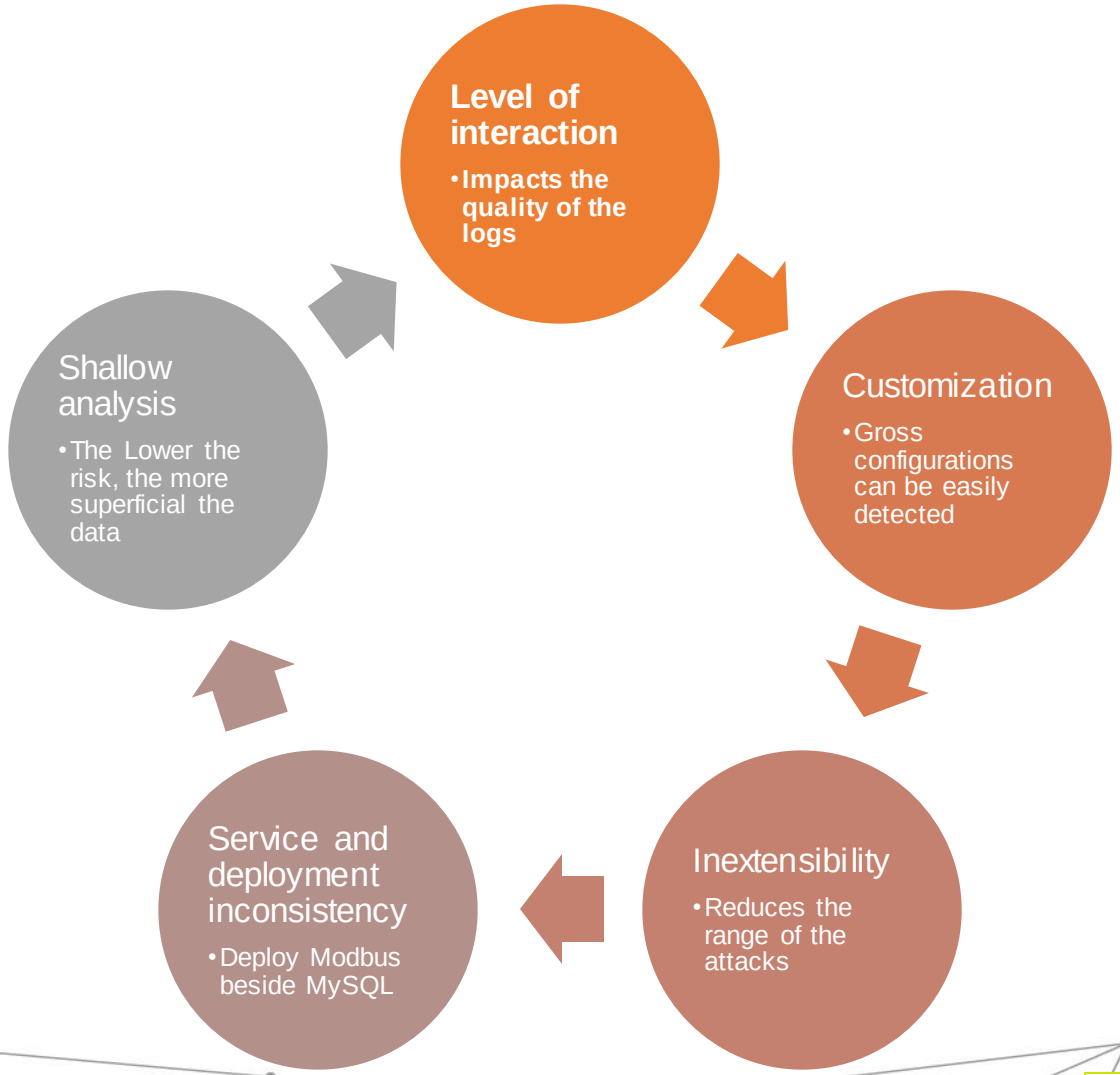
Our prior research

- Work extended using ICS honeypots (Preprint)
- Confirmed ICS / IoT traffic source correlation

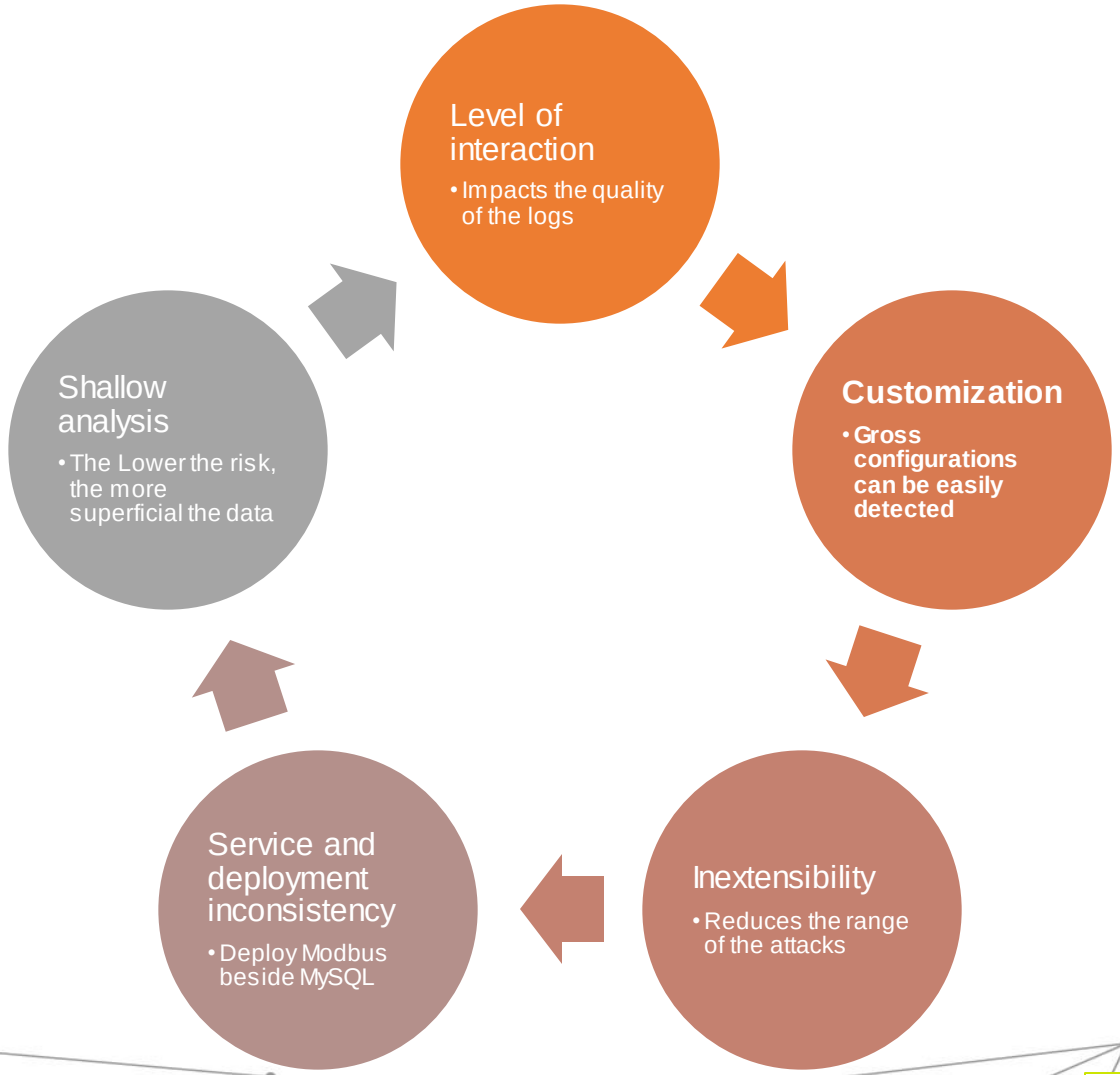


Bistarelli, Stefano, Emanuele Bosimini, and Francesco Santini. "A Report on the Security of Home Connections with IoT and Docker Honeypots." ITASEC. 2020.

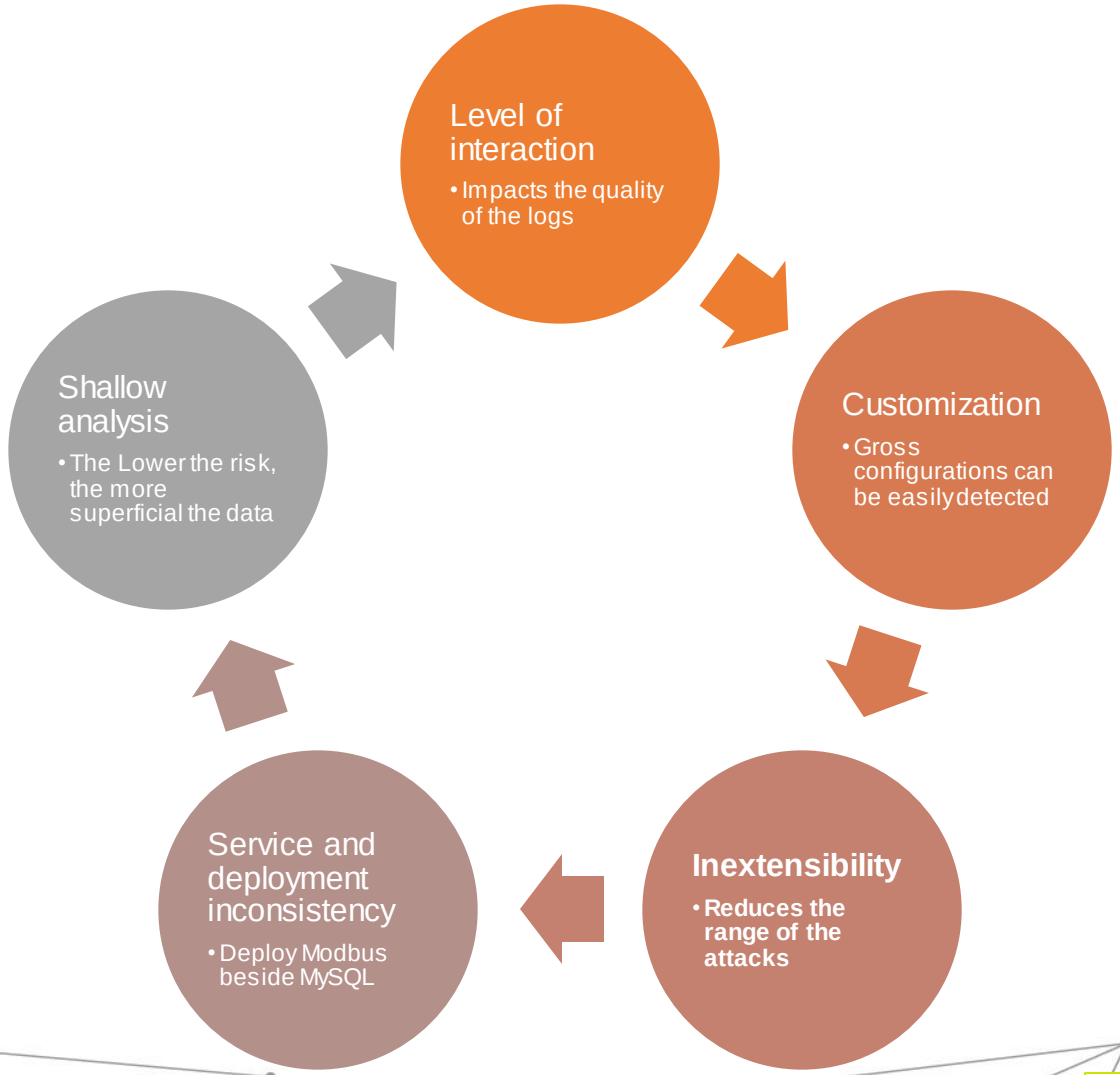
Prior research limits



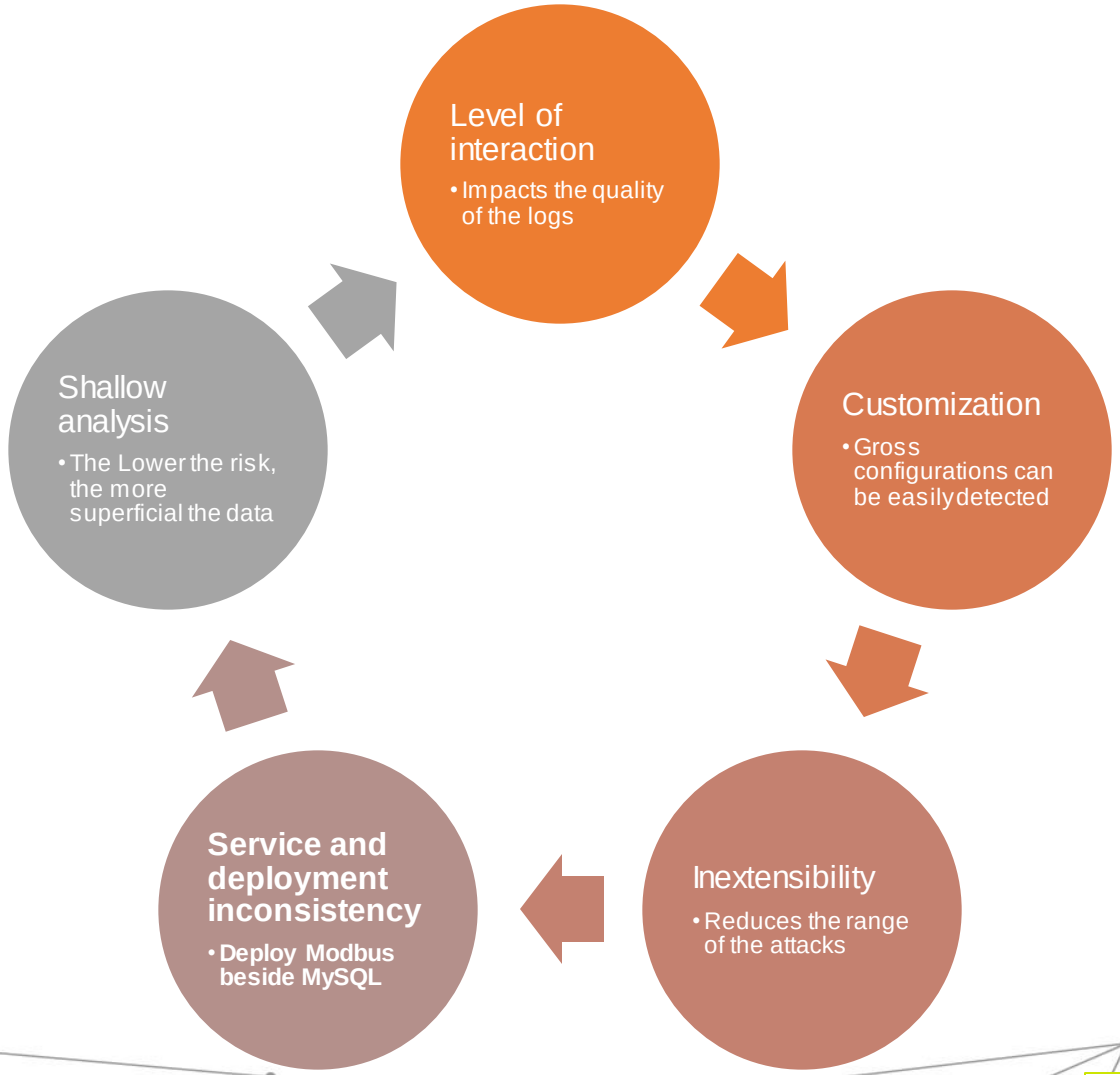
Prior research limits



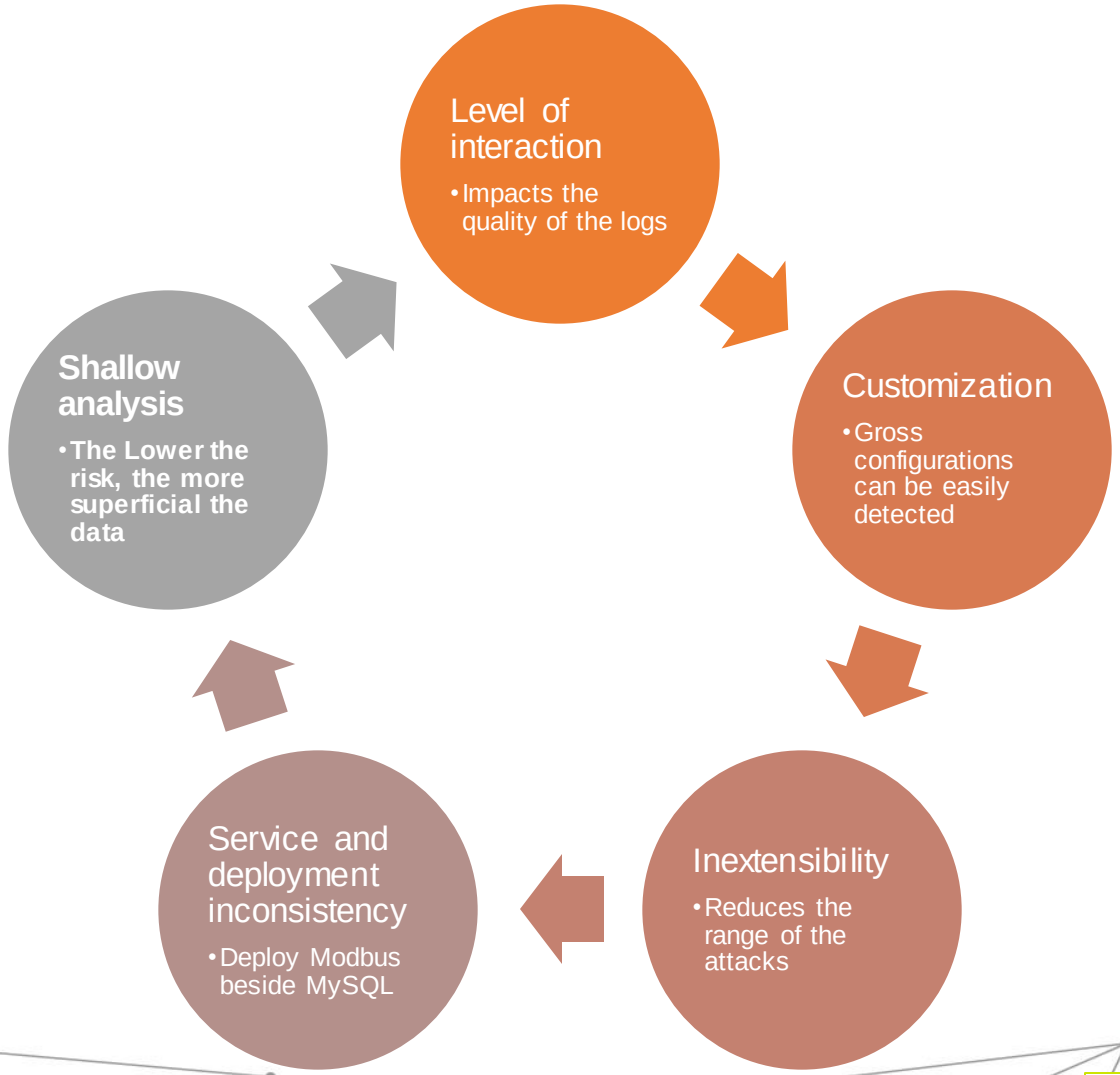
Prior research limits



Prior research limits



Prior research limits



Our proposal

Level of interaction **Medium**

Our proposal

Level of interaction	Medium
Customization	**Real PLC-device properties**

Our proposal

Level of interaction	Medium
Customization	Real PLC-device properties
Extensibility	**Through PLC templates (json/xml/csv)**

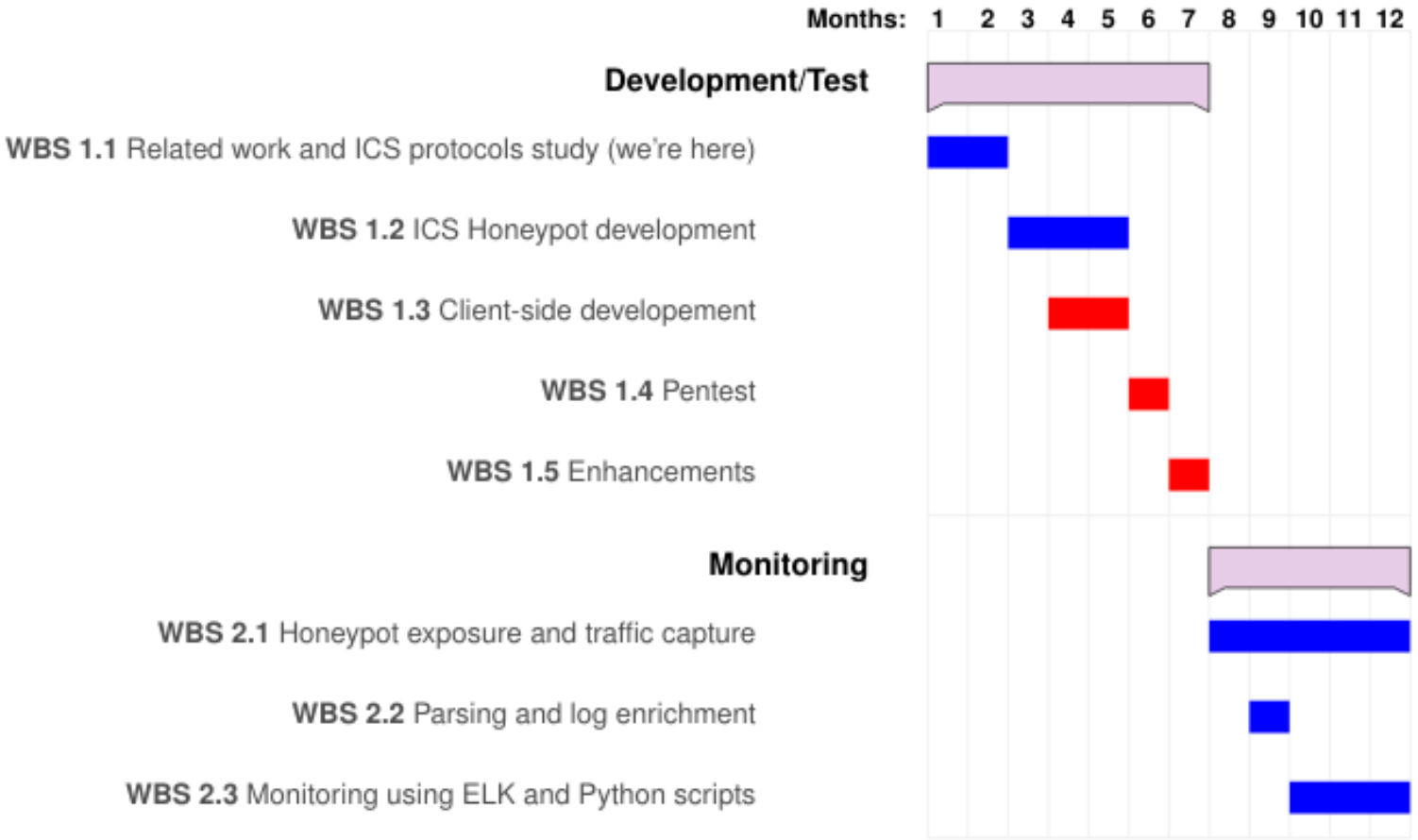
Our proposal

Level of interaction	Medium
Customization	Real PLC-device properties
Extensibility	Easy template customization (json/xml/csv)
Service and deployment consistency	**Only ICS services**

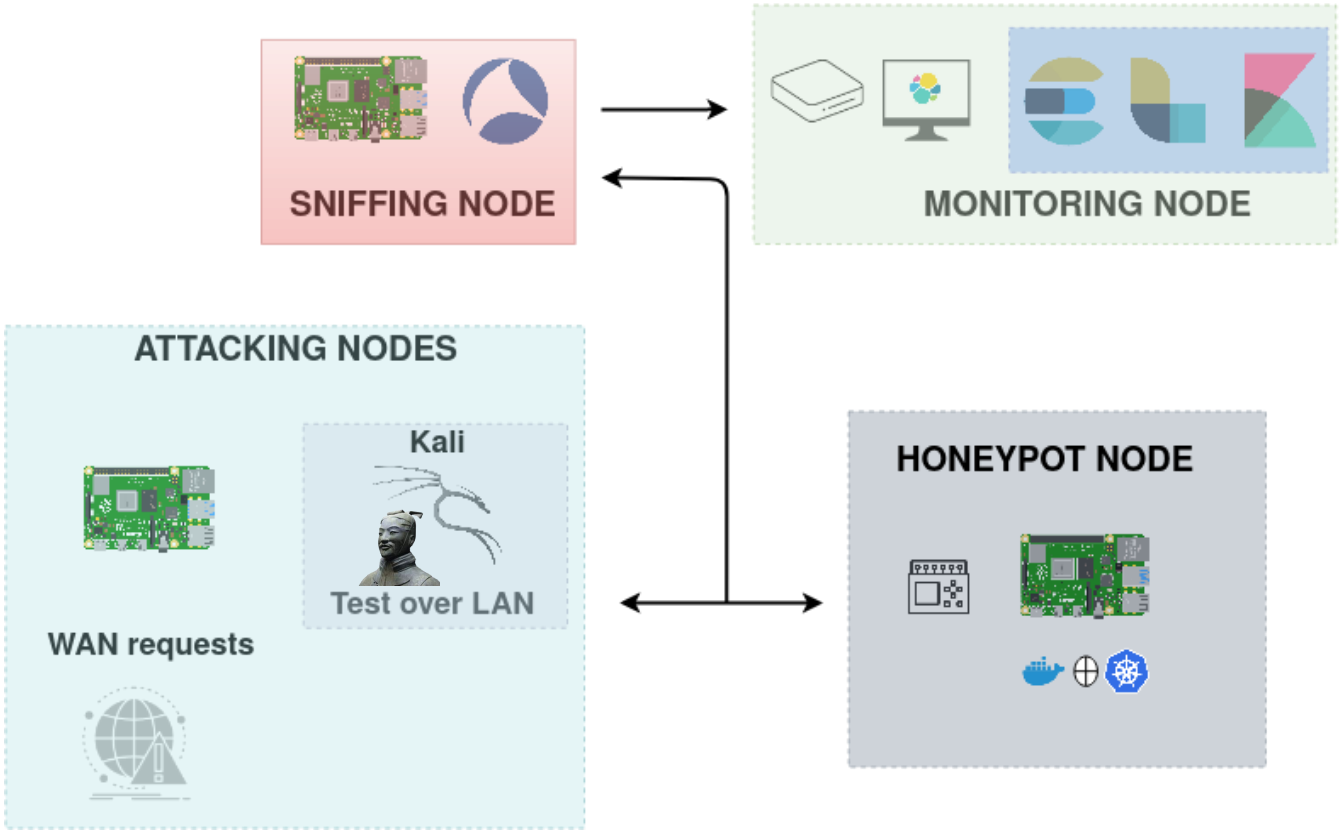
Our proposal

Level of interaction	Medium
Customization	Real PLC-device properties
Extensibility	Easy template customization (json/xml/csv)
Service and deployment consistency	Only ICS services
Sophisticated analysis	**Host/Organization behaviour, commands analysis**

Roadmap


Months: 1 2 3 4 5 6 7 8 9 10 11 12
Development/Test
WBS 1.1 Related work and ICS protocols study (we're here)
WBS 1.2 ICS Honeypot development
WBS 1.3 Client-side developement
WBS 1.4 Pentest
WBS 1.5 Enhancements
Monitoring
WBS 2.1 Honeypot exposure and traffic capture
WBS 2.2 Parsing and log enrichment
WBS 2.3 Monitoring using ELK and Python scripts

A possible architecture proposal



Challenges

- **Find**
  - any correlation between ICS services
- **Deploy**
  - the honeypot in different zones
- **Compare**
  - the results, by using also different honeypots (e.g. Conpot)
- **Determine**
  - Request types and hosts behaviour
- **Improve**
  - IDS rules (e.g. Snort, Zeek)

References

Cao, Jianhong, et al. "Dipot: A distributed industrial honeypot system." *International Conference on Smart Computing and Communication*. Springer, Cham, 2017.

Jicha, Arthur, Mark Patton, and Hsinchun Chen. "SCADA honeypots: An in-depth analysis of Conpot." *2016 IEEE conference on intelligence and security informatics (ISI)*. IEEE, 2016.

Wilhoit, Kyle, and Stephen Hilt. "The GasPot Experiment: Unexamined Perils in Using."

Ferretti, Pietro, Marcello Pogliani, and Stefano Zanero. "Characterizing background noise in ics traffic through a set of low interaction honeypots." Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy. 2019.